



CR-1382

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Sundaram et al.

Title: LOW BANDWIDTH ZERO KNOWLEDGE AUTHENTICATION  
PROTOCOL AND DEVICE

Filing Date: August 26, 2003

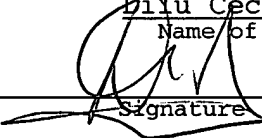
Serial Number: 10/649,855

EXPRESS MAIL mailing label number:  
EV 102067215 US

Date of Deposit: 2/4/04

I hereby certify that this correspondence is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450, on:

Dilu Cecilia Zhang  
Name of Depositor

  
Signature

\* \* \*

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Pursuant to 37 C.F.R. §1.56(a), Applicant hereby cites the following documents (copies enclosed) listed on the attached copy of Form PTO-1449.

This Information Disclosure Statement is filed in accordance with the paragraph of 37 CFR §1.97 checked below:

X 1.97(b) This Information Disclosure Statement is filed:

- (1) Within three months of the filing date of a national application; OR
- (2) Within three months of the date of entry of the national stage of an international application; OR
- (3) Before the mailing of a first Office Action on the merits.

No fee or certification is required.

     1.97(c) This Information Disclosure Statement is filed after the period specified in paragraph (b) above, but before the mailing date of either:

- (1) A Final Action under 37 CFR 1.113; OR
- (2) A Notice of Allowance under 37 CFR 1.311;

AND is accompanied by either:

(check one)

\_\_\_\_\_ the Certification under 37 CFR  
1.97(e) as set out below; OR

\_\_\_\_\_ the fee of \$240.00 under 37 CFR  
1.17(p).

\_\_\_ 1.97(d) This Information Disclosure Statement is filed  
after the mailing date of either:

(1) a Final action under 37 CFR 1.113; OR

(2) A Notice of Allowance under 37 CFR 1.311;

BUT before payment of the Issue Fee, AND is accompanied  
by:

(1) the Certification under 37 CFR 1.97(e) as  
set out below; AND

(2) Petition is hereby made under 37 CFR  
1.97(d) for consideration of this  
Information Disclosure Statement; AND,

(3) Authorization to charge the petition fee  
of \$130.00 as set out in 37 CFR 1.17(i).

If this Information Disclosure Statement is being filed  
under 37 CFR 1.97(c) or 1.97(d), the undersigned Attorney hereby  
certifies that:

— each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing date of this Statement;

or

— no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, or to the knowledge of the undersigned Attorney after making reasonable enquiry, was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing date of this Statement.

CR-1382

Authorization is hereby given to charge the indicated fee(s)  
to Deposit Account No. 50-0749.

Please charge any additional fee due for this paper to  
Deposit Account No. 50-0749.

Respectfully submitted,

MITSUBISHI ELECTRIC RESEARCH LABORATORIES

By: 

Andrew J. Curtin  
Reg. No. 48,485  
Attorney for Assignee

Mitsubishi Electric Research Laboratories, Inc.  
201 Broadway  
Cambridge, Massachusetts 02139  
(617) 621-7539

Customer No. 022199

Enclosures

~

Form PTO-1449  
(modified 2/91)U.S. DEPT OF COMMERCE  
Patent and Trademark OfficeAttorney Docket Number:  
CR-1382Serial Number:  
10/649,855**INFORMATION DISCLOSURE CITATION**

(Use several sheets if necessary)

Applicant:  
Sundaram et al.Filing date:  
August 26, 2003

Group art area:

**U.S. PATENT DOCUMENTS**

Examiner Initial	Patent number	Date	Name	Class	Sub- class	Filing date if appropriate

**FOREIGN PATENT DOCUMENTS**

	Document number	Date	Country	Class	Subclass	Translation	
						YES	NO

**OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)**

1.	Cramer R., and Shoup V., "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," Advances in Cryptology-CRYPTO '98, pp. 13-25 (1998).
2.	Guillou L. C., and Quisquater J. -J., "A practical zero knowledge protocol fitted to security microprocessor minimizing both transmission and memory," EUROCRYPT '88, pp. 123-128 (1988).
3.	Guillou L. C., and Ugon M., "Smart card: a highly reliable and portable security device," Advances in Cryptology-CRYPTO '86.
4.	LaMacchia B. A., and Odlyzko A. M., "Computation of discrete logarithms in prime fields," Designs, Codes and Cryptography, vol. 1, pp. 46-62 (1991).
5.	Morris R., and Thompson K., "Password security: a case history," Communications of the ACM, vol. 22, pp. 594-597 (1979).
6.	Quisquater J. -J., Guillou L., and Berson T., "How to explain zero knowledge protocols to your children," Advances in Cryptology-CRYPTO '89, LNCS 435, pp. 628-631 (1989).

Examiner:

Date Considered:

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP §609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.